ORIGINAL

DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY
BAHRAIN
FPO AE 09834-2800

NSABAHRAININST 3070.1A
10
3 Jun 04

U.S. NAVAL SUPPORT ACTIVITY BAHRAIN INSTRUCTION 3070.1A

Subj: OPERATION SECURITY PLAN

Ref: (a) NWP-4 (Rev A)

Encl: (1) OPSEC Terminology
(2) Essential Elements of Friendly Information

1. Purpose. To promulgate policy and procedures for the Operations Security Program at U.S. Naval Support Activity (NSA) Bahrain.

2. Cancellation. ADMINSUPUINST 3070.1.

3. Definition. Operation Security Plan (OPSEC) constitutes those actions considered necessary and appropriate to deny the enemy information concerning planned, ongoing, or completed operations and thus deny to an adversary a tactical or strategic advantage. OPSEC is the protection of military operations and activities resulting from the identification and subsequent elimination or control of intelligence indicators susceptible to hostile exploitation. Other definitions are provided in enclosure (1).

4. Responsibility

a. The Commanding Officer will:

(1) Appoint an OPSEC officer in writing to manage the Command OPSEC program.

(2) Conduct anticipatory (as required) and current OPSEC planning and use OPSEC measures to preserve essential secrecy for operations and other activities conducted or supported by the command.

b. The OPSEC officer will:

(1) Evaluate OPSEC recommendations submitted to determine their feasibility with regard to resource and operational effectiveness.

ORIGINAL

(2) Provide support regarding implementation of countermeasures.

(3) Identify/develop Essential Elements of Friendly Information (EEFI) and Command Security Objectives. Reference (a) and enclosure (2) apply.

(4) Identify vulnerabilities to foreign intelligence collection.

(5) Provide OPSEC advice and assistance where required.

(6) Request Communications Security (COMSEC) monitoring as required.

(7) Provide OPSEC training.

(8) Be responsible for implementing OPSEC Program procedures.

5. OPSEC environment. The following describes NSA Operations Security Status:

a. Automated Data Processing Security. Hardware/software resources are protected by physical security elements (i.e. controlled access, secure storage areas and appropriate clearance of personnel).

b. Physical Security. The Security Officer is responsible for physical security for the command. Physical security at NSA includes controlled access and movement control per Physical Security Regulations.

c. Information Security. Classified material is handled only by properly authorized personnel. The distribution, documentation, maintenance, and necessary destruction of classified material takes place under rigidly controlled conditions per established procedures.

d. Personnel Security. All personnel; military, civil service, and contractors employed at NSA have security clearances appropriate to the highest level of data handled. All access is controlled on a need-to-know basis.

e. Communications/Electronics Security. Access to COMSEC related material is authorized only for appropriately cleared/designated personnel. Electronic processing systems processing level one; Confidential, Secret, or Top Secret material will operate under TEMPEST certification or TEMPEST waiver issued by Commander, Naval Security Group Activity Bahrain.

6. Training

a. The OPSEC Officer will brief all newly assigned military and civil service personnel on OPSEC philosophy, organization, and command, responsibilities at scheduled indoctrinations.

b. Continuing awareness of OPSEC will be accomplished through Government Military Training, Plan of the Week note, and the sharing at staff meetings of OPSEC related problems/ solutions and lessons learned.

c. Training will be conducted on proper Beadwindow procedures in relation to EEFI violations. Enclosure (2) refers to the EEFI list, which will be placed within sight of all non-secure voice nets at NSA Bahrain.

7. Action. NSA Bahrain OPSEC Officer will consider initiatives for improving the OPSEC posture of the command.

J. M. SMITH

Distribution: (NSABAHRAININST 5216.1Q)
List I

OPSEC TERMINOLOGY

1. Operations Security. The process of denying adversaries information about friendly capabilities and intentions by identifying controlling, and protecting indicators associated with planning and conducting military operations and other activities.

2. Military Deception. Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives.

3. Cover. Military deceptions to cause misinterpretation of and minimal concern or curiosity about observables that are generated by operations and other activities. Covers are targeted not only at adversaries but also at random observers and sometimes at personnel with access to classified information.

4. Essential Elements of Friendly Information (EEFI). Key questions about U.S. intentions and military capabilities likely to be asked by opposing planners and decision makers.

a. EEFI lists. Were developed to identify specific items of information which, if acquired by an adversary, will degrade the security of military operations, special projects etc. A standard EEFI list enclosure (2) is provided.

b. Beadwindow Procedures. A real-time procedure which brings to the immediate attention of circuit operators the fact that an EEFI disclosure enclosure (2) has occurred. The report also serves to alert other operators on the net of the EEFI disclosure and thus acts as an educational aid. Although Beadwindow is to be used on all U.S. Navy Voice Communications, these procedures can also be applied to phone conversations where a STU III (Secure Terminal Unit) is not available or even in our day-to-day conversations with non-cleared personnel. Awareness of disclosures, identified by the EEFI List, on any voice net, or conversation is important and should be brought to the attention of the military unit in question.

5. Appreciations. Assumptions, estimates and facts about an opponent's intentions, military capabilities and current activities used in planning and decision making.

a. Desired Appreciations. Adversary estimates that result in adversary intentions, military capabilities, and current activities to friendly advantage.

b. Essential Secrecy. Specific unknowns or uncertainties about friendly intentions, military capabilities, and current activities to friendly advantage.

c. Harmful Appreciations. Assumptions about the adversary or estimates to provide for unknowns or uncertainties which result in mis-guessing adversary's intentions, military capabilities, and current activities.

6. Sources of Information:

a. Secret Sources and Methods. Personnel, documents, material, and other matters that are knowledgeable of or embody classified information and abilities to process classified matters. Secret sources and methods result from weaknesses in security protection for classified matters and hostile success in exploiting those weaknesses through espionage, human source elicitation, theft, crypto analysis and code breaking.

b. Open Sources of Information. Oral, documentary, pictorial, and physical materials accessible by the public. Open sources of information result from administrative actions and include such things as: technical articles, public affairs releases, contract awards, budgets, speeches, awards, schedules, flight plans, biographies, job descriptions, motel reservations, manifests and sales to foreign countries.

7. Categories of Information:

a. Controlled Information. Information conveyed or denied to an adversary to evoke desired appreciations.

b. Protected Information. Information accorded protection prescribed for classified matters.

c. Indicators. Data obtained from open sources of information or derived from detectable activities that can be synthesized or interpreted with respect to background knowledge to make estimates. Actions that convey indicators and must be carried out to plan, prepare and execute operations and other activities while exploitable by foreign intelligence organizations which are called observable.

d. Deception Means. There are three categories of deception means: Administrative, physical, and technical, used to conveyor deny information to foreign countries.

(1) Administrative Means. Capabilities to convey and deny to a foreign country oral, documentary, pictorial, or other physical evidence through the open and secret sources of information it uses to gather information.

(2) Physical Means. Capabilities to convey and deny to a foreign country information derivable form foreign observation, imagery, or active sensor surveillance of physical matters on activities.

(3) Technical Means. Capabilities to convey and deny to a foreign country information through electronic and acoustic countermeasures, the emission or suppression of nuclear particles and other techniques that effect phenomena exploited by sensors.

8. Protection for Classified Matters:

a. Administrative. Personnel security; procedures for marking, accounting for, disposing of and handling classified matters; application of need to know principle; foreign disclosure; and transfer-of-technology decisions.

b. Physical. Guarding classified matters during transport or in spaces or areas where classified matters are located or discussed to deny unauthorized personnel access; executing physical activities inside spaces where they cannot be observed or photographed; physically covering classified matters.

c. Technical. Encryption; codes; tempest; ADP security; sound proofing; shielding enclosures so as not to emit classified signals.

9. OPSEC Measures. Means of controlling and protecting indicators so as to provide sufficiently for essential secrecy.

a. Control of Open Sources of Information and Detectable Activities. Selecting what, whether, when, where and how administrative, physical, and technical actions are carried out so indicators are eliminated or are not accessible to adversaries in time to be used effectively in adversary planning and decision making.

b. Protective Measures. The use of military deceptions (including covers) to explain observables, deceptions and Countermeasures against collection systems; includes physical force against collectors.

10. Service Operations and Other Activities

a. Service Operations. Such things as: generation of naval forces in periods of hostilities, provisions of logistics and administrative support to operating forces, sea trials, shakedown cruises, unit training, fleet exercises, salvage and recovery, departmental intelligence collection and oceanographic surveys.

b. Other Activities. Such things as: maintenance, mailing spare parts and mail, developmental, operational and follow-on tests, tests of tactics and techniques, conferences, contracting, budgeting, congressional testimony, mobilization, continuity of Department of the Navy functioning at all levels of conflict.

ORIGINAL



ESSENTIAL ELEMENTS of FRIENDLY INFORMATION (EEFI)

01 Friendly or enemy position, movement or intended movement: position; course; speed; altitude; or destination of any air, sea, or ground element unit or force.

02 Friendly or enemy capabilities or limitations: force composition or identity; capabilities; limitations or significant casualties to special equipment, weapon systems, sensors, units, or personnel; percentages of fuel or ammunition remaining.

03 Friendly or enemy operations, intentions, progress or results: operational or logistic intentions; assault objectives; mission participants; flying programs; mission situation reports; results of friendly or enemy operations.

04 Friendly or enemy EW/EMCON intentions, progress or results: Intention of employ ECM; results of friendly or enemy ECM objectives of ECMS; results of friendly or enemy ECCM; results of ESM; present or intended EMCON policy; equipment affected by EMCON policy.

05 Friendly or enemy key personnel: movement or identity of friendly or enemy flag officers; distinguished visitors; unit commanders; movements of key maintenance personnel indicating equipment limitations.

06 Friendly or enemy COMSEC locations: linkage of codes or code words with plain language; compromise of changing frequencies or linkage with line numbers; circuit designators; linkage of changing call signs with previous call signs or units; compromise of encrypted/classified call signs; incorrect authentication procedure.

07 Inappropriate transmission: Information requested, transmitted, or about to be transmitted which should not be passed on the subject circuit because it either requires greater security protection or is not appropriate for the purpose for which the circuit is provided.